(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 677 949 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
28.05.2003 Bulletin 2003/22

(51) Int Cl.[7]: **H04N 1/44**

(21) Application number: **95103972.6**

(22) Date of filing: **17.03.1995**

(54) **Method for controlling copyright of encrypted digital data**

Verfahren um die Urheberrechte von verschlüsselten numerischen Daten zu kontrollieren

Procédé pour contrôler les droits d'auteur de données numériques chiffrées

(84) Designated Contracting States:
DE FR GB

(30) Priority: **01.04.1994 JP 6488994**

(43) Date of publication of application:
18.10.1995 Bulletin 1995/42

(60) Divisional application:
01111936.9 / 1 133 163

(73) Proprietor: **MITSUBISHI CORPORATION**
Chiyoda-ku, Tokyo 100-0005 (JP)

(72) Inventors:
- **Saito, Makato**
  Tama-shi, Tokyo (JP)
- **Momiki, Shunichi**
  Higashimurayama-shi, Tokyo (JP)

(74) Representative: **Pfenning, Meinig & Partner**
Mozartstrasse 17
80336 München (DE)

(56) References cited:
EP-A- 0 398 645
EP-A- 0 581 227
EP-A- 0 590 763
EP-A- 0 649 074

- **RESEARCH DISCLOSURE, no. 335, March 1992 EMSWORTH GB, page 219 XP 000301128 'Encryption of information to be recorded so as to prevent unauthorised playback'**

EP 0 677 949 B1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to a process for data copyright control for controlling copyright of digital data encrypted by using a crypt key and supplied from a database to a user. A preferred embodiment relates to an application of the method to a multi-media system.

Prior Art

[0002] In the information-oriented society of today, a database system is being propagated, in which it is possible to use various types of data, stored independently by each computer in the past, by connecting the computers by communication lines. In such a database system, the information handled so far has been classical type coded information, which can be processed by computer and contains relatively few amount of information and monochrome binary data such as facsimile information at the most, and it is not possible to handle the data containing relatively large amount of information such as natural picture or animation.

[0003] A system for encryption of an information signal to be recorded on a record carrier such, that the recorded information cannot be reproduced unless a key code is available to the user of said reproduction apparatus is known for Example, from Research Disclosure (1992) March, No. 335, Emsworth, GB, p. 219.

[0004] With rapid progress of digital processing technique for various types of electric signals, a technique for digital processing of picture signals other than binary data, handled only as analog signals in the past, is under development.

[0005] By digitizing the picture signal, it becomes possible to handle picture signal such as television signal by computer, and attention is now focused on "multi-media system" , which can simultaneously handle the data processed by computers and also digitized picture data, as a technique of the future.

[0006] Because the picture data contains overwhelmingly large amount of information compared with character data and audio data, it is difficult to store, transfer or process these data by computer.

[0007] For this reason, it has been designed to compress and expand these picture data, and several standards for compression/expansion of picture data have been prepared. Among them, the following standards have been established as common standards: JPEG (Joint Photographic image coding Experts Group) standards for still picture, H.261 standards for television conference, MPEG1 (Moving Picture image coding Experts Group 1) standards for picture accumulation, and MPEG2 standards to cope with the current television broadcasting and high definition television broadcasting.

[0008] By these new techniques, it is now possible to transmit digital picture data at real time.

[0009] In analog data, which have been widely used in the past, the control of copyright occurring in these processings did not become an important issue because quality of these analog data is deteriorated each time when these data are stored, copied, edited or transferred. However, quality deterioration of digital data does not occur even when these are repeatedly stored, copied, fabricated or transferred, and the management and control of copyright occurring in the processings are an important problem.

[0010] Up to present, there has been no adequate method for management and control of copyright for digital data. It has been merely managed and controlled by copyright law or by contracts. In the copyright law, merely compensation for digital type sound and picture recording devices have been prescribed.

[0011] In the use of database systems, it is possible not only to refer to the content thereof but also effectively utilize the obtained data by storing, copying or editing, and also to transfer the edited data to other persons or to the database and to register as a new data.

[0012] In the conventional type database system, only character data have been handled, while, in a multi-media system, sound data and picture data, which are originally analog data, are digitized and used as database in addition to the data such as characters used as database.

[0013] Under such circumstances, it is important how to handle copyright of the data, which have been used as database. However, there has been no means for copyright management and control, in particular, on copying, edit, transfer, etc.

[0014] A system for executing copyright control by obtaining a permit key from a key control center via public telephone line for using encrypted data has been disclosed in Japanese Patent Application 4-199942 (GB-A-2269302, DE-A-4323569 and FR-A-2697394) and Japanese Patent Application 4-289074 (GB-A-2272823, DE-A-4335835 and FR-A-2697707) of the present inventors, and a device for this purpose has been disclosed in the Japanese Patent Application 4-276941 (GB-A-2272822, DE-A-4334931 and FR-A-2697124).

[0015] It is the problem of the present invention to provide a method for controlling copyright in display (including the process of sound), storage, copying, edit and transfer of digital data in a database system including real time transmission of digital picture by developing the inventions of the prior applications further.

[0016] The problem is solved by the processes of claim 1 and 12. Further preferred embodiments may be taken from the subclaims.

[0017] For the control of copyright, it is essential in the database system, to which the present invention is applied,
to transmit one or more, when necessary, among copyright information, copyright control message and a program for controlling copyright, in addition to a key which

allows to use to users who wish to use encrypted data.

[0018] The copyright control message is displayed on a screen and advises or warns the user in case the data are being utilized other than the conditions of user's request or permission. The copyright control program watches and controls in order that the data are not utilized beyond the conditions of the user's request or the permission.

[0019] The copyright control program, the copyright information and the copyright control message are supplied together with a permit key in some cases, or they are supplied together with data in some other cases. Or, a part of them is supplied together with the permit key, and other part is suppied with the data.

[0020] For the data, the permit key, the copyright control message, the copyright information and the copyright control program, there are the following three cases: a case where these are transmitted with encrypted, and upon using, the encryption is decrypted, a case where they are transmitted with encrypted and remain in encrypted except being decrypted only when they are displayed, and a case where they are not encrypted at all.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021]

Fig. 1A and Fig. 1B each represents examples of display pictures of messages of the present invention;

Fig. 2A and Fig. 2B each represents a drawing for showing television signals; and

Fig. 3A to Fig. 3J each represents concept of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0022] In the following, description will be given on embodiments of the present invention.

[0023] In the prior patent applications mentioned above, it is described under the assumption that a permit key obtaining route is different from a data obtaining route as shown in Fig. 3A, and the permit key is obtained from a key control center via public telephone line. However, if a charging method is determined, it is possible to obtain the permit key via a communication system, through which the database is supplied.

[0024] In the system of the prior patent applications, it is assumed that the permit key for secondary exploitation is used for distribution of the data for secondary exploitation, and secondary exploitation of storage, copying, edit, transfer, etc. of data is not included in the assumption. Also, it is assumed that the data is distributed only inside LAN, to which the users belong, and distribution to outside is not assumed. Therefore, this system is not adequate to cope with the secondary exploitation unless the users are conscious in esteeming the copyright.

[0025] To cope with various forms of the secondary exploitation as described above, a plurality of the permit keys are prepared to match each form of use, and no utilization is possible unless there is a permit key suitable for the desired form of use.

[0026] As the forms of use of database, there are display, storage, copying, edit, transfer, etc. Simply speaking, the permit keys suitable for these forms of use should be prepared.

[0027] However, in case it is desired to execute several forms of use at the same time, it is necessary to obtain a plurality of permit keys. If failing to obtain the permit keys, the desired form of use may not be executed.

[0028] To avoid such situations, a permit key can be used, which makes it possible to execute several forms of use, for example, permit keys, which are hierarchical and an upper-level key also fulfills the function of a lower-level key.

[0029] For example, from lower-level to upper-level is defined as display < storage < copying < edit < transfer. By the display permit key, only display can be executed. Display and storage can be executed by the storage permit key. Display, storage and copying can be executed by the copying permit key. Display, storage, copying and edit can be executedby the edit permit key, and display, storage, copying, editand transfer can be executed by the transfer permit key.

[0030] In the prior patent application, i.e. in Japanese Patent Application 4-276941 (GB-932102.5, DE-P4334931.5 and FR-9312285), the present inventors have proposed asystem, in which a plurality of encrypted data, each of which is encrypted by a plurality of different crypt keys, are recorded as encrypted, and data are decrypted when uing, i.e. a system where storage permit key is used as the lowest level key.

[0031] By applying this system, it is possible to set from lower-level to upper-level in the order of storage < copying <transfer < display < edit. Specifically, it is set in such manner that storage can be executed by a storage permit key, storage and copying can be executed by a copying permit key, storage, copying and transfer can be executed by a transfer permit key, storage, copying, transfer and display can be executed by a display permit key, and storage, copying, transfer, display and edit can be executed by a edit permit key.

[0032] In this system, storage, copying and transfer are placed at lower level than display because, even when storage, copying and transfer are executed on the data, which cannot be displayed, it is difficult and meaningless to utilize such data, and it is necessary to execute display in order to utilize the data.

[0033] This hierarchical arrangement is best suited to a system, in which encrypted data are supplied and are utilized using a permit key.

[0034] The permit key is usually offered to the user on

pay basis. Therefore, except the case where it is allowed to utilize the data limitlessly, the number of use times of the permit key is limited to one time or several times if it is necessary to limit the number of use times.

[0035] Because the data can be used if there is a permit key, it is possible to use the data beyond the range of permission if the permit key is duplicated or falsified. To prevent this, the permit key is encrypted.

[0036] The use of data includes storage, display, copying, edit, transfer, etc. thereof, which are necessary to be allowed or prohibited.

[0037] In case it is necessary to limit the number of use times or to limit forms of use, it is desirable to display a message for such purpose.

[0038] In case the information on copyright is falsified, the data supplier or the user may undergo damage, and this must be prevented.

[0039] To ensure completeness on copyright control, information on original copyright and information for secondary and tertiary copyright on edition of data are given to the data.

[0040] The above copyright control is executed by the copyright control program.

[0041] In conventional type database sysem, the data itself is offered in completely defenseless state. Therefore, the copyright control can be executed only when data is taken out from the database. In the subsequent copyright control, there is no other way but to rely on conscience of the users and to take necessary measures when the data are utilized beyond the permission range of use.

[0042] For this reason, as described in the prior patent application, i.e. in Japanese Patent Application 4-276941 (GB-932102.5, DE-P4334931.5 and FR-9312285), the data supplied from the database are left in encrypted state, and storage is executed under this condition. In addition, copying and transfer are also executed in encrypted state. And decrypting is performed only in display and edit, and these are controlled by the copyright control program.

[0043] In so doing, it is impossible to use the data beyond the permitted range.

[0044] In this case, the copyright control porgam may be integrated with the data or may be encrypted.

[0045] Because the copyright control program is encrypted and the permit key decrypts the copyright control program and because the copyright control program decrypts and encrypts the data, the data are encrypted twofold.

[0046] In this case, if a key unique to the data is added to the copyright control program to encrypt the data, it is impossible to decrypt the data in case the copyright control program is separated.

[0047] In this copyright control program, in case the data are stored, copied or transferred even within the permitted range, and if these are executed after the data and the copyright program have been encrypted, it is impossible to use the data in inadequate manner.

[0048] In case an operator inadequately uses a computer program and, as a result, the computer does not respond any more or computer operation is stopped, error message is displayed so that the operator may understand the cause. Similarly, if a user of the database erroneously uses beyond the permitted range of the permit key and, as a result, the computer does not respond any more or operation is stopped, the user cannot understand the cause.

[0049] In such case, a copyright control message is displayed just as an error message is displayed by the copyright control program.

[0050] The display of the copyright control message as described above also fulfills the function of warning in case the user intentionally uses the data beyond the range of use of the permit key.

[0051] In general, various programs are incorporated in ROM in side the equipment which the user uses, or the programs are supplied from software. In case the programs are incorporated in ROM, there is no possibility that the programs are changed, but the equipment to be used is limited to those, in which the ROM is incorporated. On the other hand, in case the programs are supplied from software, there is no limitation if the programs are transferred, but there is a possibility that the programs may be altered.

[0052] The database is utilized by various users using various types of devices. Therefore, in case the programs to control the copyright are supplied as software, it is necessary to cope with various types of devices, and there must not be the possibility to change the program.

[0053] Therefore, to prevent such trouble, the copyright control program should be encrypted.

[0054] In this case, as a matter of fact, it is necessary to modify the program according to the device, which the user uses. In such case, a program to translate the copyright control program is provided in communication software of the device which the user uses, and the copyright control progam is translated by the translation program of the copyright control program so that it suits the device.

[0055] Even when the permit key itself for using the database as described above may be more complicated by encryption, data size of several tens of bites is sufficient at the most. Therefore, the time required for transmitting the permit key is far shorter than one second. In other words, even when charged public telephone line is used and other information is transmitted together with the permit key, the increase of cost is negligible.

[0056] Therefore, when transmitting the permit key as shown in Fig. 3B utilizing surplus time, the copyright control program can be transmitted.

[0057] The copyright control program can be supplied together with the permit key and also together with the data as shown in Fig. 3C.

[0058] In this case, the copyright control program is supplied together with the data, and the entire data uti-

lization is placed under control of the copyright control program. For example, it is set in such manner that the data supplied in encrypted state cannot be decrypted unless the copyright program supplied with it is used, and in case there is no such copyright control program, the data cannot be used.

[0059] In so doing, the control of copyright is further reinforced.

[0060] Further, if the copyright control program is integrally united with the data, copyright control is further reinforced.

[0061] The following are some examples of the copyright control message:

"Need a display permit key."
"Need a storage permit key."
"Need a copying permit key."
"Need an edit permit key."
"Need a transfer permit key. "

Some other examples are:

"Display unavailable."
"Storage unavailable."
"Copy unavailable. "
"Edit unavailable. "
"Transfer unavailable. "

[0062] These copyright control messages are displayed alone as shown in Fig. 1A or in combination as shown in Fig. 1B.

[0063] Next, description will be given on supply of the copyright control message.

[0064] To display the copyright control message, the message must be stored in memory of the device, which the user uses. The memory in the device is classified to ROM and RAM.

[0065] The method to store in ROM is a reliable method, but there is a limitation to the device to be used because the user must use the ROM, where the copyright control messages are stored.

[0066] As the methods to store in RAM, there are a method to supply together with the permit key, a method to supply together with the copyright control program, and a method to supply together with the data. It is needless to say that, when the permit key and the copyright control program are supplied at the same time, the copyright control message can be supplied at the same time.

[0067] The copyright control message is not effective unless an adequate one is displayed. For this reason, the copyright control message cannot play its original role when the message is changed in such manner that no substantial content is displayed, or further, its content is null to be displayed. To prevent such trouble, the message is encrypted.

[0068] The display of the copyright control message is executed by the copyright control program. The modes of display are as follows: when it is tried to perform an operation with no adequate key available, a corresponding message is displayed; all messages corresponding to operation, available for the current permit key, are displayed, if it is tried to perform an oreration without available permit key.

[0069] The copyright control message is supplied together with the permit key as shown in Fig. 3D or together with the data as shown in Fig. 3E.

[0070] The copyright control message is transmitted by transmitting all messages or only the necessary messages required. In the former case, the quantity of information is plenty, but security is high. In the latter case, the quantity of information is relatively few, but security is low.

[0071] It is desirable that the copyright control message cannot be separated from the data just as in the case of the copyright control program, by the means for integrating it with copyright control program.

[0072] To display the copyright on printed matter, the name of the author and the date are used. The copyright of the database is displayed by entering information such as the name of the author and the date.

[0073] As described above, edit and up-load of edited data are included in the use of the data in the database. Specifically, the presence of secondary data, which is edited from the data, i.e. a work of authorship, is recognized. To ensure the copyright of the data in this context, it is necessary to store the information on original authorship and secondary authorship together with the data.

[0074] For this purpose, in case use of the data other than down-load and display of the data is executed, copyright information including the information on the operator is stored together with the data as history in addition to the copyright information up to that moment.

[0075] In this case, it is set in such manner that only the person who controls the database can put the original author ship to database as primary data, and all data handled by other than the person in charge of database control are as secondary data, and the control of history can be further reinforced.

[0076] When the copyright information is separated from the data, which is a work of authorship, it becomes extremely difficult to recognize the copyright. Thus, it is necessary to set that the copyright information cannot be separated from the data.

[0077] To disable the copyright information to separate from the data, there are a method to integrate the data with the copyright information or a method to make the data not utilizable unless copyright information is available, just as in the case of the copyright control program or the case of the copyright control message as described above.

[0078] First, description will be given on the method to integrate the data with the copyright information.

[0079] The data handled by computer comprises a file header indicating data name and size and a file body,

which is main body of the data. Therefore, to integrate the data with the copyright information there are methods to integrate the copyright information with the file header, to integrate the copyright information with the file body, and to take other means for the purpose.

[0080] Among these methods, the method to integrate the copyright information with file header is available even without file header in case of character information expressed by character code. Thus, it is a simple method but not very reliable. Also, because the capacity of the file header is not so high, it is not sufficient in case there are a large amount of copyright information.

[0081] Digital picture data and digital sound data are grouped, and a header is added to this group. The copyright information can be integrated to this group header.

[0082] However, there is a problem of header capacity similar to the case of file header in this case.

[0083] As the method to integrate the copyright information with the file body, one way is to add it for each edited data, and another is to add it all together.

[0084] In case of adding the copyright information for each edited data, the copyright information is added to each data, which is edited by cut and paste procedure. This case is not only complicated but disadvantageous in that the entire file data becomes too big.

[0085] If the picture data is indicated the copyright of original authorship, it is easy to confirm to which data corresponds, and thus, it is not always necessary to add the copyright information to each minimum unit of the edited data.

[0086] It is also possible to write the copyright information into the copyright program. In this method, it is difficult to manipulate the copyright information if it is written in the copyright control program integrated with the data asalready described.

[0087] In case the data is a picture signal, it is necessary to have synchronization signal data in order to define scanning line, field and frame. This synchronization signal has high redundancy and is generally turned to code of variable-length. Thus, the copyright information can be mixed with the code of variable-length. The number of scanning lines is 480 in case of VGA standards. By utilizing this, a considerable quantity of information can be mixed in it.

[0088] In case the picture data is animated picture, it is possible to write sufficient quantity of copyright informationin this method. However, if the picture data is a still picture edited by cut and paste procedure, there may be no space enough to add the copyright control information.

[0089] Fig. 2A and Fig. 2B each represents a structure of a signal of analog type television and that of a signal of digital type television. Fig. 2A represents the case of analog television, and Fig. 2B shows the case of digital television.

[0090] The signal other than picture data such as multiplex teletext signal in analog television is inserted by utilizing vertical retrace interval, and horizontal retrace interval is not utilized.

[0091] In contrast, in digital television, it is possible for copyright control program or other multiplex teletext signal to enter into horizontal scanning data or into vertical scanning data.

[0092] As a method to integrate the copyright information with data, one way is to write the copyright information into the data itself, and another is to write it into control code.

[0093] As the data used in computer, there is control code for controlling communication system or computer system in addition to the data to be displayed on screen or used for some operation, and this control code cannot be seen by the user. Therefore, if the copyright information is written into the control code, the copyright information thus written does not cause trouble in the use by the user.

[0094] It is also possible to enter into the file of the computer using the technique of computer virus without affecting the operation itself.

[0095] The copyright information may be supplied together with the permit key as shown in Fig. 3F or may be supplied together with data as shown in Fig. 3G.

[0096] Attention has been focused in recent years on digital signature. Using a private key which only the person concerned knows and a public key which other persons also know, digital signature is prepared from the private key and from the data of file size based on the document. If the document is changed, the change can be confirmed by the private key, and the content of the document can be seen at any time by the other persons using the public key. Thus, this offers very high security.

[0097] The data of computer can be changed without leaving any trace. For this reason, if the copyright of the data is infringed without being noticed, this may not be known to the author, or a user, who uses the data without knowing that the content of the data has been changed, may be suffered some damage.

[0098] To prevent such trouble, digital signature is attached to the data, which may be changed, and the damage to the copyright owner or the user can be avoided.

[0099] The "permit key", "copyright control program ", "copyright control message ", and "copyright information " can be combined in any way as necessary to actualize the method for controlling database copyright.

[0100] Also, it is possible to design in such manner that only a part of the data of the copyright control program, the copyright control message or the copyright information is supplied together with the permit key as shown in Fig. 3H, 31 and 3J and that the other part is supplied together with the data so that the part supplied as the permit key and the part supplied together with the data are combined together and the function as a complete permit key serves after they have been combined together.

[0101] In so doing, it is possible to give the function

of the permit key to the copyright program and copyright control message, and higher security is ensured.

Claims

1. Process for data copyright control for controlling copyright of digital data encrypted by using a crypt key and supplied from a database to a user, **characterized by** the steps of:

   supplying a utilization permit key from a key control center to said user; wherein said utilization permit key is a display permit key for displaying said digital data, an edit permit key for editing said digital data, a storage permit key for storing said digital data, a copy permit key for copying said digital data and/or a transfer utilization permit key for transferring said digital data;
   decrypting said encrypted digital data using said permit key by said user; and
   displaying, editing, storing, copying or transfer of said digital data by said user.

2. Process for data copyright control according to Claim 1, **characterized by** giving digital signature to said digital data.

3. Process for data copyright control according to Claims 1 or 2, **characterized by** using at least one of a copyright control program for controlling copyright of said digital data, a copyright information for copyright of said digital data or a copyright control message for use of said digital data on copyright in addition to each of said permit keys.

4. Process for data copyright control according to Claim 3, **characterized by** storing, copying or transferring said copyright information together with said digital data if said digital data is stored, copied or transferred.

5. Process for data copyright control according to Claim 3 or 4, **characterized by** adding history information for editing, copying or transferring of said digital data to said copyright information if said digital data is edited, copies or transferred.

6. Process for data copyright control according to one of the Claims 1, 2, 3, 4 or 5, **characterized by** encrypting said display permit key, said edit permit key, said storage permit key, said copy permit key and/or said transfer permit key.

7. Process for data copyright control according to Claim 6, **characterized by** decrypting said encrypted digital data by said copyright control program.

8. Process for data copyright control according to one of Claims 3, 4, 5, 6 or 7, **characterized by** encrypting said copyright control program.

9. Process for data copyright control according to one of Claims 3, 4, 5, 6, 7 or 8, **characterized by**: supplying said copyright control program, said copyright information or said copyright control message together with said utilization permit key.

10. Process for data copyright control according to one of Claims 3, 4, 5, 6, 7 or 8, **characterized by** :

    supplying said copyright control program, said copyright information or said copy right control message together with said encrypted digital data from the database; and
    supplying said utilization permit key from said key control center.

11. Process for data copyright control according to one of Claims 3, 4, 5, 6, 7, or 8, **characterized by**:

    supplying a part of said copyright program, said copyright information or said control message together with said encrypted digital data from the database; and
    supplying another part of said copyright control program, said copyright information or said copyright control message together with said permit key from said key control center.

12. Process for data copyright control for controlling copyright of digital data encrypted by using a crypt key and supplied from a database to a user, **characterized by** the steps of:

    supplying a utilization permit key from a key control center to said user; wherein said utilization permit key is a display permit key for displaying said digital data, an edit permit key for editing said digital data, a storage permit key for storing said digital data, a copy permit key for copying said digital data and/or a transfer permit key for transferring said digital data;

    displaying, editing, storing, copying or transferring said digital data by using said utilization permit key by said user; wherein said encrypted digital data is decrypted when said digital data is displayed and edited, and

    encrypting again said digital data when said user stores, copies or transfers said digital data.

13. Process for data copyright control according to Claim 12, **characterized by** giving a digital signature to said digital data.

14. Process for data copyright control according to Claims 12 or 13, **characterized by** using at least one of: copyright control program for controlling copyright of said digital data, copyright information for copyright of said digital data and a copyright control message for using said digital data on copyright in addition to each of said permit keys.

15. Process for data copyright control according to Claim 14, **characterized by** storing, copying or transferring said copyright information if said digital data is stored, copied or transferred.

16. Process for data copyright control according to Claims 14 or 15, **characterized by** adding history information for editing, copying or transferring of said digital data to said copyright information if said digital data is edited, copied or transferred.

17. Process for data copyright control according to one of the Claims 12, 13, 14, 15 or 16, **characterized by** encrypting said display permit key, said edit permit key, said storage permit key, said copy permit key and/or said transfer permit key.

18. Process for data copyright control according to Claim 17, **characterized by** decrypting the encrypted digital data by said copyright control program.

19. Process for data copyright control according to one of the Claims 14, 15, 16, 17 or 18, **characterized by** encrypting said copyright control program.

20. Process for data copyright control according to one of the Claims 14, 15, 16, 17, 18 or 19, **characterized by** supplying said copyright control program, said copyright information or said copyright control message together with said permit key.

21. Process for data copyright control according to one of the Claims 14, 15, 16, 17, 18 or 19, **characterized by**
supplying said copyright control program, said copyright information or said copyright control message together with said encrypted digital data from the database; and
supplying said permit key from said key control center.

22. Process for data copyright control according to one of Claims 14, 15, 16, 17, 18 or 19, **characterized by** supplying a part of said copyright control program, said copyright information or said copyright control message together with the encrypted digital data from the database; and
supplying another part of said copyright control program, said copyright information or said copyright control message together with said permit key from said key control center.

Patentansprüche

1. Verfahren für die Kontrolle des Urheberrechts von Daten zum Kontrollieren des Urheberrechts von verschlüsselten digitalen Daten durch Verwendung eines Schlüssels, die von einer Datenbank zu einem Benutzer geliefert werden, **gekennzeichnet durch** die Schritte:

   - Liefern eines Benutzungserlaubnisschlüssels von einem Schlüsselkontrollzentrum zu dem Benutzer; worin der Benutzungserlaubnisschlüssel ein Anzeigeerlaubnisschlüssel für die Anzeige der digitalen Daten, ein Aufbereitungserlaubnisschlüssel für die Aufbereitung der digitalen Daten, ein Speichererlaubnisschlüssel für die Speicherung der digitalen Daten, ein Vervielfältigungserlaubnisschlüssel für die Vervielfältigung der digitalen Daten und/oder ein Übertragungsbenutzungs-Erlaubnisschlüssel für die Übertragung der digitalen Daten ist;
   - Entschlüsseln der verschlüsselten digitalen Daten und Verwendung des Erlaubnisschlüssels **durch** den Benutzer; und
   - Anzeigen, Aufbereiten, Speichern, Vervielfältigen oder Übertragen der digitalen Daten **durch** den Benutzer.

2. Verfahren für die Kontrolle des Urheberrechts von Daten nach Anspruch 1,
dadurch gekennzeichnet, dass den digitalen Daten eine digitale Unterschrift gegeben wird.

3. Verfahren für die Kontrolle des Urheberrechts von Daten nach Anspruch 1 oder 2,
gekennzeichnet durch die Verwendung von zumindest einem Urheberrechtskontrollprogramm zum Kontrollieren des Urheberrechts der digitalen Daten von Urheberrechtsinformationen über das Urheberrecht an den digitalen Daten oder von einer Urheberrechts-Kontrollnachricht zur Verwendung der urheberrechtsgeschützten digitalen Daten zusätzlich zu jedem der Erlaubnisschlüssel.

4. Verfahren für die Kontrolle des Urheberrechts von Daten nach Anspruch 3,
gekennzeichnet durch Speichern, Vervielfältigen oder Übertragen der Urheberrechtsinformationen zusammen mit den digitalen Daten, wenn die digitalen Daten gespeichert, vervielfältigt oder übertragen werden.

5. Verfahren für die Kontrolle des Urheberrechts von Daten nach Anspruch 3 oder 4,
gekennzeichnet durch Hinzufügen von Vergan-

genheitsinformationen für die Aufbereitung, das Vervielfältigen oder das Übertragen der digitalen Daten zu den Urheberrechtsinformationen, wenn die digitalen Daten aufbereitet, vervielfältigt oder übertragen werden.

6. Verfahren für die Kontrolle des Urheberrechts von Daten nach einem der Ansprüche 1, 2, 3, 4 oder 5, **gekennzeichnet durch** Verschlüsseln des Anzeigeerlaubnisschlüssels, des Aufbereitungserlaubnisschlüssels, des Speichererlaubnisschlüssels, des Vervielfältigungserlaubnisschlüssels und/oder des Übertragungserlaubnisschlüssels.

7. Verfahren für die Kontrolle des Urheberrechts von Daten nach Anspruch 6, **gekennzeichnet durch** Entschlüsseln der verschlüsselten digitalen Daten **durch** das Urheberrechtskontrollprogramm.

8. Verfahren für die Kontrolle des Urheberrechts von Daten nach einem der Ansprüche 3, 4, 5, 6 oder 7, **gekennzeichnet durch** Verschlüsseln des Urheberrechtskontrollprogramms.

9. Verfahren für die Kontrolle des Urheberrechts von Daten nach einem der Ansprüche 3, 4, 5, 6, 7 oder 8, **gekennzeichnet durch**:

   - Liefern des Urheberrechtskontrollprogramms, der Urheberrechtsinformationen oder der Urheberrechtskontrollnachricht zusammen mit dem Benutzungserlaubnisschlüssel.

10. Verfahren für die Kontrolle des Urheberrechts von Daten nach einem der Ansprüche 3, 4, 5, 6, 7 oder 8, **gekennzeichnet durch**:

    - Liefern des Urheberrechtskontrollprogramms, der Urheberrechtsinformationen oder der Urheberrechtskontrollnachricht zusammen mit den verschlüsselten digitalen Daten von der Datenbank; und
    - Liefern des Benutzungserlaubnisschlüssels von dem Schlüsselkontrollzentrum.

11. Verfahren für die Kontrolle des Urheberrechts von Daten nach einem der Ansprüche 3, 4, 5, 6, 7 oder 8, **gekennzeichnet durch**:

    - Liefern eines Teils des Urheberrechtsprogramms, der Urheberrechtsinformationen oder der Kontrollnachricht zusammen mit den verschlüsselten digitalen Daten von der Datenbank; und
    - Liefern eines anderen Teils des Urheberrechtskontrollprogramms, der Urheberrechtsinformationen oder der Urheberrechtskontrollnachricht zusammen mit dem Erlaubnisschlüssel von dem Schlüsselkontrollzentrum.

12. Verfahren für die Kontrolle des Urheberrechts von Daten zum Kontrollieren des Urheberrechts von digitalen Daten, die durch Verwendung eines Schlüssels verschlüsselt sind und von einer Datenbank zu einem Benutzer geliefert wurden, **gekennzeichnet durch** die Schritte:

    - Liefern eines Benutzungserlaubnisschlüssels von einem Schlüsselkontrollzentrum zu dem Benutzer;
      worin der Benutzungserlaubnisschlüssel ein Anzeigeerlaubnisschlüssel für die Anzeige der digitalen Daten, ein Aufbereitungserlaubnisschlüssel für die Aufbereitung der digitalen Daten, ein Speichererlaubnisschlüssel für die Speicherung der digitalen Daten, ein Vervielfältigungserlaubnisschlüssel für die Vervielfältigung der digitalen Daten und/oder ein Übertragungserlaubnisschlüssel für die Übertragung der digitalen Daten ist;
    - Anzeigen, Aufbereiten, Speichern, Vervielfältigen oder Übertragen der digitalen Daten **durch** Verwendung des Benutzungserlaubnisschlüssels **durch** den Benutzer; worin die verschlüsselten digitalen Daten entschlüsselt werden, wenn die digitalen Daten angezeigt und aufbereitet werden; und
    - Wiederverschlüsseln der digitalen Daten, wenn der Benutzer die digitalen Daten speichert, vervielfältigt oder überträgt.

13. Verfahren für die Kontrolle des Urheberrechts von Daten nach Anspruch 12, **dadurch gekennzeichnet, dass** den digitalen Daten eine digitale Unterschrift gegeben wird.

14. Verfahren für die Kontrolle des Urheberrechts von Daten nach Anspruch 12 oder 13, **gekennzeichnet durch** Verwendung zumindest eines von: einem Urheberrechtskontrollprogramm zum Kontrollieren des Urheberrechts der digitalen Daten, von Urheberrechtsinformationen über das Urheberrecht an den digitalen Daten und einer Urheberrechtskontrollnachricht zur Verwendung der digitalen Daten über das Urheberrecht zusätzlich zu jedem der Erlaubnisschlüssel.

15. Verfahren für die Kontrolle des Urheberrechts von Daten nach Anspruch 14, **gekennzeichnet durch** Speichern, Vervielfältigen oder Übertragen der Urheberrechtsinformationen, wenn die digitalen Daten gespeichert, vervielfältigt

oder übertragen werden.

16. Verfahren für die Kontrolle des Urheberrechts von Daten nach Anspruch 14 oder 15, **gekennzeichnet durch** Hinzufügen von Vergangenheitsinformationen für die Aufbereitung, Vervielfältigung oder Übertragung der digitalen Daten zu den Urheberrechtsinformationen, wenn die digitalen Daten aufbereitet, vervielfältigt oder übertragen werden.

17. Verfahren für die Kontrolle des Urheberrechts von Daten nach einem der Ansprüche 12, 13, 14, 15 oder 16, **gekennzeichnet durch** Verschlüsseln des Anzeigeerlaubnisschlüssels, des Aufbereitungserlaubnisschlüssels, des Speichererlaubnisschlüssels, des Vervielfältigungserlaubnisschlüssels und/oder des Übertragungserlaubnisschlüssels.

18. Verfahren für die Kontrolle des Urheberrechts von Daten nach Anspruch 17, **gekennzeichnet durch** Entschlüsseln der verschlüsselten digitalen Daten **durch** das Urheberrechtskontrollprogramm.

19. Verfahren für die Kontrolle des Urheberrechts von Daten nach einem der Ansprüche 14, 15, 16, 17 oder 18, **gekennzeichnet durch** Verschlüsseln des Urheberrechtskontrollprogramms.

20. Verfahren für die Kontrolle des Urheberrechts von Daten nach einem der Ansprüche 14, 15, 16, 17, 18 oder 19, **gekennzeichnet durch** die Lieferung des Urheberrechtskontrollprogramms, der Urheberrechtsinformationen oder der Urheberrechtskontrollnachricht zusammen mit dem Erlaubnisschlüssel.

21. Verfahren für die Kontrolle des Urheberrechts von Daten nach einem der Ansprüche 14, 15, 16, 17, 18 oder 19, **gekennzeichnet durch**

    - Liefern des Urheberrechtskontrollprogramms, der Urheberrechtsinformationen oder der Urheberrechtskontrollnachricht zusammen mit den verschlüsselten digitalen Daten von der Datenbank; und
    - Liefern des Erlaubnisschlüssels von dem Schlüsselkontrollzentrum.

22. Verfahren für die Kontrolle des Urheberrechts von Daten nach einem der Ansprüche 14, 15, 16, 17, 18 oder 19, **gekennzeichnet durch**

    - Liefern eines Teils des Urheberrechtskontrollprogramms, der Urheberrechtsinformationen oder der Urheberrechtskontrollnachricht zusammen mit den verschlüsselten digitalen Daten von der DAtenbank; und
    - Liefern eines anderen Teils des Urheberrechtskontrollprogramms, der Urheberrechtsinformationen oder der Urheberrechtskontrollnachricht zusammen mit dem Erlaubnisschlüssel von dem Schlüsselkontrollzentrum.

Revendications

1. Procédé de contrôle de droits d'auteur de données afin de contrôler les droits d'auteur de données numériques chiffrées en utilisant une clé de chiffrage et acheminées d'une base de données à un utilisateur, **caractérisé par** les étapes suivantes:

   délivrance d'une clé d'autorisation d'utilisation d'un centre de contrôle de clés audit utilisateur, dans laquelle ladite clé d'autorisation d'utilisation est une clé d'autorisation d'affichage pour afficher lesdites données numériques, une clé d'autorisation d'édition pour éditer lesdites données numériques, une clé d'autorisation de stockage pour stocker lesdites données numériques, une clé d'autorisation de copie pour copier lesdites données numériques et/ou une clé d'autorisation de transfert pour transférer lesdites données numériques;

   déchiffrage desdites données numériques chiffrées par utilisation de ladite clé d'autorisation par ledit utilisateur; et

   affichage, édition, stockage, copie ou transfert desdites données numériques par ledit utilisateur.

2. Procédé de contrôle de droits d'auteur de données selon la revendication 1, **caractérisé par** l'affectation d'une signature numérique auxdites données numériques.

3. Procédé de contrôle de droits d'auteur de données selon la revendication 1 ou 2, **caractérisé en ce qu'**on utilise au moins l'un des éléments suivants : un programme de contrôle de droits d'auteur pour contrôler les droits d'auteur desdites données numériques, des informations de droits d'auteur pour les droits d'auteur desdites données numériques ou un message de contrôle de droits d'auteur pour un usage desdites données numériques avec ses droits d'auteur en plus de chacun desdits clés d'autorisation.

4. Procédé de contrôle de droits d'auteur de données selon la revendication 3, **caractérisé en ce qu'**on stocke, on copie ou on transfère lesdites informations de droits d'auteur conjointement avec lesdites données numériques si lesdites données numériques sont stockées, copiées ou transférées.

5. Procédé de contrôle de droits d'auteur de données selon la revendication 3 ou 4, **caractérisé en ce qu'**on ajoute des informations historiques pour l'édition, la copie ou le transfert desdites données numériques auxdites informations de droits d'auteur si lesdites données numériques sont éditées, copiées ou transférées.

6. Procédé de contrôle de droits d'auteur de données selon l'une quelconque des revendications 1, 2, 3, 4 ou 5, **caractérisé en ce que** l'on chiffre ladite clé d'autorisation d'affichage, ladite clé d'autorisation d'édition, ladite clé d'autorisation de stockage, ladite clé d'autorisation de copie et/ou ladite clé d'autorisation de transfert.

7. Procédé de contrôle de droits d'auteur de données selon la revendication 6, **caractérisé en ce que** l'on déchiffre lesdites données numériques chiffrées par ledit programme de contrôle de droits d'auteur.

8. Procédé de contrôle de droits d'auteur de données selon l'une quelconque des revendications 3, 4, 5, 6 ou 7, **caractérisé en ce que** l'on chiffre ledit programme de contrôle de droits d'auteur.

9. Procédé de contrôle de droits d'auteur de données selon l'une quelconque des revendications 3, 4, 5, 6, 7 ou 8, **caractérisé en ce que** l'on délivre ledit programme de contrôle de droits d'auteur, lesdites informations de droits d'auteur ou ledit message de contrôle de droits d'auteur conjointement avec ladite clé d'autorisation d'utilisation.

10. Procédé de contrôle de droits d'auteur de données selon l'une quelconque des revendications 3, 4, 5, 6, 7 et 8, **caractérisé en ce que** :

    on délivre ledit programme de contrôle de droits d'auteur, lesdites informations de droits d'auteur ou ledit message de contrôle de droits d'auteur conjointement avec lesdites données numériques chiffrées depuis la base de données; et

    on délivre ladite clé d'autorisation d'utilisation depuis ledit centre de contrôle de clés.

11. Procédé de contrôle de droits d'auteur de données selon l'une quelconque des revendications 3, 4, 5, 6, 7 et 8, **caractérisé en ce que** :

    on délivre une partie dudit programme de droits d'auteur, desdites informations de droits d'auteur ou dudit message de contrôle de droits d'auteur conjointement avec lesdites données numériques chiffrées depuis la base de données; et

    on délivre une autre partie dudit programme de contrôle de droits d'auteur, desdites informations de droits d'auteur ou dudit message de contrôle de droits d'auteur conjointement avec ladite clé d'autorisation depuis ledit centre de contrôle de clés.

12. Procédé de contrôle de droits d'auteur de données afin de contrôler les droits d'auteur de données numériques chiffrées en utilisant une clé de chiffrage et délivrées d'une base de données à un utilisateur, **caractérisé par** les étapes suivantes :

    délivrance d'une clé d'autorisation d'utilisation d'un centre de contrôle de clés audit utilisateur, dans laquelle ladite clé d'autorisation d'utilisation est une clé d'autorisation d'affichage pour afficher lesdites données numériques, une clé d'autorisation d'édition pour éditer lesdites données numériques, une clé d'autorisation de stockage pour stocker lesdites données numériques, une clé d'autorisation de copie pour copier lesdites données numériques et/ou une clé d'autorisation de transfert pour transférer lesdites données numériques,

    affichage, édition, stockage, copie ou transfert desdites données numériques par utilisation de ladite clé d'autorisation d'utilisation par ledit utilisateur, où lesdites données numériques chiffrées sont déchiffrées lorsque lesdites données numériques sont affichées et éditées, et

    chiffrage à nouveau desdites données numériques lorsque ledit utilisateur stocke, copie ou transfère lesdites données numériques.

13. Procédé de contrôle de droits d'auteur de données selon la revendication 12, **caractérisé en ce que** l'on affecte une signature numérique auxdites données numériques.

14. Procédé de. contrôle de droits d'auteur de données selon la revendication 12 ou 13, **caractérisé en ce qu'**on utilise au moins l'un des éléments suivants : un programme de contrôle de droits d'auteur pour contrôler les droits d'auteur desdites données numériques, des informations de droits d'auteur pour les droits d'auteur desdites données numériques et un message de contrôle de droits d'auteur pour l'utilisation desdites données numériques avec ses

droits d'auteur en plus de chacune desdites clés d'autorisation.

15. Procédé de contrôle de droits d'auteur de données selon la revendication 14, **caractérisé en ce qu'**on stocke, on copie ou on transfère lesdites informations de droits d'auteur si lesdites données numériques sont stockées, copiées ou transférées.

16. Procédé de contrôle de droits d'auteur de données selon la revendication 14 ou 15, **caractérisé en ce que** l'on ajoute des informations historiques pour éditer, copier ou transférer lesdites données numériques auxdites informations de droits d'auteur si lesdites données numériques sont éditées, copiées ou transférées.

17. Procédé de contrôle de droits d'auteur de données selon l'une quelconque des revendications 12, 13, 14, 15 ou 16, **caractérisé en ce que** l'on chiffre ladite clé d'autorisation d'affichage, ladite clé d'autorisation d'édition, ladite clé d'autorisation de stockage, ladite clé d'autorisation de copie et/ou ladite clé d'autorisation de transfert.

18. Procédé de contrôle de droits d'auteur de données selon la revendication 17, **caractérisé en ce que** l'on déchiffre les données numériques chiffrées par ledit programme de contrôle de droits d'auteur.

19. Procédé de contrôle de droits d'auteur de données selon l'une quelconque des revendications 14, 15, 16, 17 ou 18, **caractérisé en ce que** l'on chiffre ledit programme de contrôle de droits d'auteur.

20. Procédé de contrôle de droits d'auteur de données selon l'une quelconque des revendications 14, 15, 16, 17, 18 ou 19, **caractérisé en ce que** l'on délivre ledit programme de contrôle de droits d'auteur, lesdites informations de droits d'auteur ou ledit message de contrôle de droits d'auteur conjointement avec ladite clé d'autorisation.

21. Procédé de contrôle de droits d'auteur de données selon l'une quelconque des revendications 14, 15, 16, 17, 18 ou 19, **caractérisé en ce que**

on délivre ledit programme de contrôle de droits d'auteur, lesdites informations de droits d'auteur ou ledit message de contrôle de droits d'auteur conjointement avec lesdites données numériques chiffrées depuis la base de données; et

on délivre ladite clé d'autorisation depuis ledit centre de contrôle de clés.

22. Procédé de contrôle de droits d'auteur de données selon l'une quelconque des revendications 14, 15, 16, 17, 18 ou 19, **caractérisé en ce que** :

on délivre une partie dudit programme de contrôle de droits d'auteur, desdites informations de droits d'auteur ou dudit message de contrôle de droits d'auteur conjointement avec les données numériques chiffrées depuis la base de données; et

on délivre une autre partie dudit programme de contrôle de droits d'auteur, desdites informations de droits d'auteur ou dudit message de contrôle de droits d'auteur conjointement avec ladite clé d'autorisation depuis ledit centre de contrôle de clés.

FIG. 1A

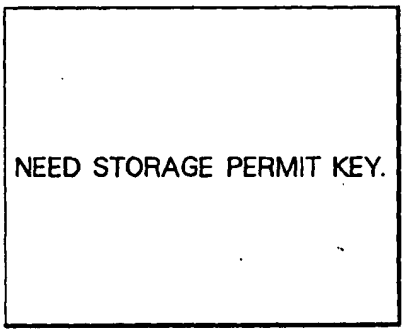

FIG. 1B

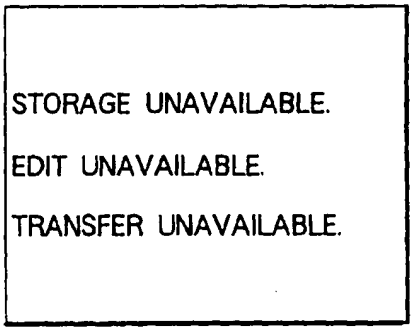

FIG. 2A

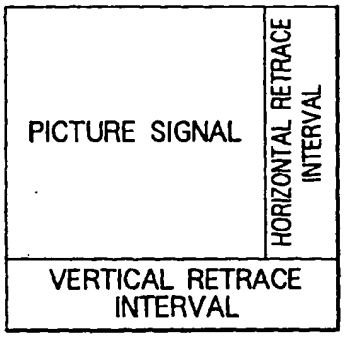

FIG. 2B

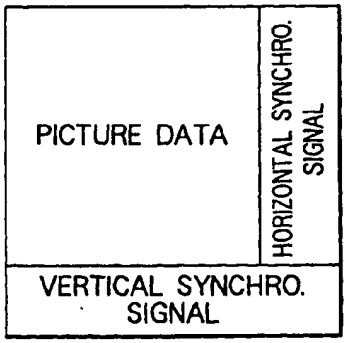

FIG. 3A

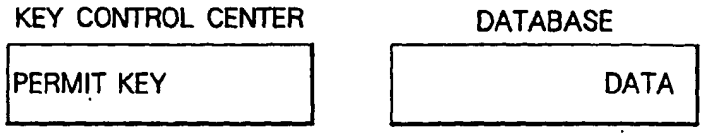

FIG. 3B

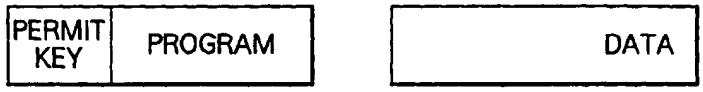

FIG. 3C

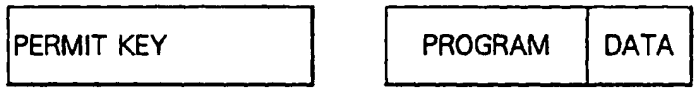

FIG. 3D

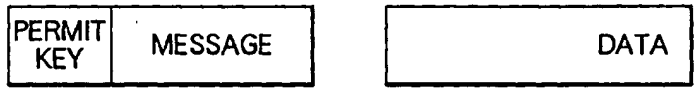

FIG. 3E

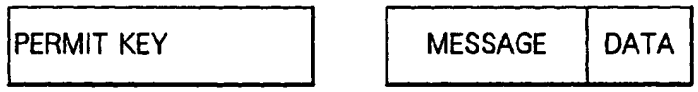

FIG. 3F

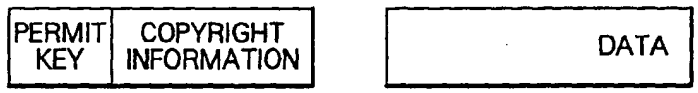

FIG. 3G

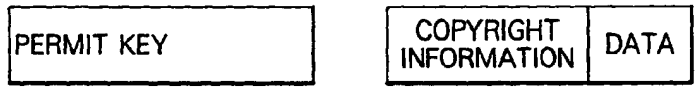

FIG. 3H

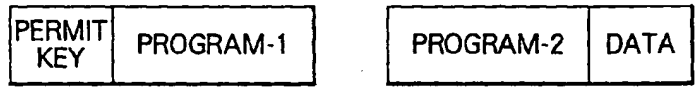

FIG. 3I

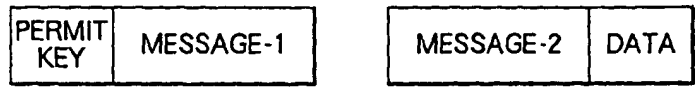

FIG. 3J